Lecture Notes in Computer Science **10436**

Commenced Publication in 1973
Founding and Former Series Editors:
Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

More information about this series at http://www.springer.com/series/7410

Joaquin Garcia-Alfaro · Guillermo Navarro-Arribas
Hannes Hartenstein · Jordi Herrera-Joancomartí (Eds.)

Data Privacy Management, Cryptocurrencies and Blockchain Technology

ESORICS 2017 International Workshops, DPM 2017 and CBT 2017, Oslo, Norway, September 14–15, 2017 Proceedings

Springer

Editors
Joaquin Garcia-Alfaro
Télécom SudParis
Evry
France

Guillermo Navarro-Arribas
Department of Information
and Communications Engineering
Autonomous University of Barcelona
Bellaterra
Spain

Hannes Hartenstein
Karlsruhe Institute of Technology
Karlsruhe
Germany

Jordi Herrera-Joancomartí
Autonomous University of Barcelona
Bellaterra
Spain

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-319-67815-3 ISBN 978-3-319-67816-0 (eBook)
DOI 10.1007/978-3-319-67816-0

Library of Congress Control Number: 2017953409

LNCS Sublibrary: SL4 – Security and Cryptology

Printed on acid-free paper

This Springer imprint is published by Springer Nature
The registered company is Springer International Publishing AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Foreword from the DPM 2017 Program Chairs

This volume contains the proceedings of the 12th Data Privacy Management International Workshop (DPM 2017), held in Oslo, Norway, during September 14–15, 2017, in conjunction with the 22nd European Symposium on Research in Computer Security (ESORICS) 2017. The DPM series started in 2005 when the first workshop took place in Tokyo (Japan). Since then, the event has been held in different venues: Atlanta, USA (2006); Istanbul, Turkey (2007); Saint Malo, France (2009); Athens, Greece (2010); Leuven, Belgium (2011); Pisa, Italy (2012); Egham, UK (2013); Wroclaw, Poland (2014); Vienna, Austria (2015); and Crete, Greece (2016).

The aim of DPM is to promote and stimulate the international collaboration and research exchange in areas related to the management of privacy-sensitive information. This is a very critical and important issue for organizations and end-users. It poses several challenging problems, such as translation of high-level business goals into system-level privacy policies, administration of sensitive identifiers, data integration and privacy engineering, among others.

For this workshop edition we received 51 submission, and each one was evaluated on the basis of significance, novelty, and technical quality. The Program Committee, formed by 41 members, performed an excellent task and with the help of an additional 18 referees all submissions went through a careful review process (three or more reviews per submission). In the end, 16 full papers were accepted for presentation at the event. In addition, the program was completed with a keynote talk given by Vicenç Torra (University of Skövde, Sweden) on integral privacy (privacy models and disclosure risk).

We would like to thank everyone who helped organize the event, including all the members of the Organizing Committee of both ESORICS and DPM 2017.

Our gratitude goes also to Pierangela Samarati, Steering Committee Chair of the ESORICS Symposium, for all her arrangements to make possible the satellite events, and Socratis Katsikas, Workshops Chair of ESORICS 2017. Last but by no means least, we thank all the DPM 2017 Program Committee members, additional reviewers, all the authors who submitted papers, and all the workshop attendees.

Finally, we want to acknowledge the support received from the sponsors of the workshop: Institut Mines-Telecom (Telecom SudParis), CNRS Samovar UMR 5157 (R3S team), Universitat Autonoma de Barcelona, UNESCO Chair in Data Privacy, Universitat Rovira i Virgili, and project TIN2014-55243-P from the Spanish MINECO.

August 2017

Joaquin Garcia-Alfaro
Guillermo Navarro-Arribas

Organization

12th International Workshop on Data Privacy Management — DPM 2017

Program Committee Chairs

Joaquin Garcia-Alfaro	Telecom SudParis, Paris-Saclay University, France
Guillermo Navarro-Arribas	Universitat Autònoma de Barcelona, Spain

Program Committee

Günes Acar	KU Leuven, Belgium
Jordi Casas-Roma	Universitat Oberta de Catalunya, Spain
Jordi Castella-Roca	Universitat Rovira i Virgili, Spain
Frederic Cuppens	Telecom Bretagne, France
Nora Cuppens-Boulahia	Telecom Bretagne, France
Josep Domingo-Ferrer	Universitat Rovira i Virgili, Spain
Christian Duncan	Quinnipiac University, USA
Sara Foresti	Università degli Studi di Milano, Italy
Sebastien Gambs	Université du Québec à Montréal, Canada
Paolo Gasti	New York Institute of Technology, USA
Marit Hansen	Unabhängiges Landeszentrum für Datenschutz, Germany
Jordi Herrera-Joancomarti	Universitat Autònoma de Barcelona, Spain
Masahiro Inuiguchi	Osaka University, Japan
Marc Juarez	KU Leuven, Belgium
Florian Kammueller	Middlesex University London, UK
Hiroaki Kikuchi	Meiji University, Japan
Evangelos Kranakis	Carleton University, Canada
Maryline Laurent	Telecom SudParis, Paris-Saclay University, France
Giovanni Livraga	Università degli Studi di Milano, Italy
Javier Lopez	University of Malaga, Spain
Brad Malin	Vanderbilt University, USA
Chris Mitchell	Royal Holloway, UK
Tarik Moataz	Brown University, USA
Refik Molva	EURECOM, France
Anna Monreale	University of Pisa, Italy
Jordi Nin	BBVA Data & Analytics, Spain

Melek Önen	EURECOM, France
Cristina Pérez-Solà	Universitat Autònoma de Barcelona, Spain
Silvio Ranise	FBK, Security and Trust Unit, Trento, Italy
Kai Rannenberg	Goethe University, Germany
Yves Roudier	Université de Nice, France
Pierangela Samarati	Università degli Studi di Milano, Italy
David Sanchez	Universitat Rovira i Virgili, Spain
Claudio Soriente	Telefonica Research and Development, Spain
Matthias Templ	Vienna University of Technology, Austria
Vicenç Torra	University of Skövde, Sweden
Yasuyuki Tsukada	Kanto Gakuin University, Japan
Alexandre Viejo	Universitat Rovira i Virgili, Spain
Jens Weber	University of Victoria, Canada
Lena Wiese	University of Göttingen, Germany
Nicola Zannone	Eindhoven University of Technology, The Netherlands

Steering Committee

Josep Domingo-Ferrer	Universitat Rovira i Virgili, Spain
Joaquin Garcia-Alfaro	Telecom SudParis, Paris-Saclay University, France
Guillermo Navarro-Arribas	Universitat Autònoma de Barcelona, Spain
Vicenç Torra	University of Skövde, Sweden

Additional Reviewers

Carles Anglès-Tafalla
Monir Azraoui
Sergi Delgado-Segura
Gerardo Fernandez
José Maria de Fuentes
Akos Grosz
Paolo Guarda
Daniel Homann
Ibrahim Lazrig
Wanpeng Li
Fatma Al Maqbali
Ana Nieto
Jose A. Onieva
Alfredo Rial
Sara Ricci
Ruben Rios
Jordi Ribes-González
Hari Siswantoro

Foreword from CBT 2017 Program Chairs

This volume contains the proceedings of the First International Workshop on Cryptocurrencies and Blockchain Technology (CBT 2017) held in Oslo, Norway, on September 14, 2017, in conjunction with the 22nd European Symposium on Research in Computer Security (ESORICS) 2017.

Since the appearance of Bitcoin in 2009, a plethora of new cryptocurrencies and other blockchain-based systems have been proposed and deployed. While some of them are slightly different copies of Bitcoin, others propose interesting improvements or new usages of the underlying blockchain technology. Owing to their construction as blockchain-based systems, security and dependability aspects need to be rigorously designed and analyzed. The goal of the CBT workshop is to provide a forum for researchers in this area to carefully analyze current systems and propose new ones in order to create a scientific background for the solid development of new cryptocurrencies and blockchain technology systems.

In response to the call for papers, we received 27 submissions that were carefully reviewed by the Program Committee comprising 15 members and by additional reviewers. Each submission received at least three reviews. The Program Committee selected six papers as full papers (resulting in an acceptance rate of about 22%) and four short papers for presentation at the workhop. The selected papers cover aspects of identity management, smart contracts, soft- and hardforks, proof-of-works and proof-of-stake as well as on network layer aspects and the application of blockchain technology for secure concert/event ticketing.

Furthermore, the workshop was enhanced by the keynote offered by Prof. Roger Wattenhofer, a talk that was made possible thanks to the sponsorship of Blockchain Inc.

We would like to thank all the authors who submitted papers to CBT 2017 and the Program Committee and the additional reviewers who worked hard to review the submissions and discussed the final program. We would also like to thank the ESORICS workshop chair Sokratis Katsikas and his team as well as the ESORICS organizers for putting faith in us and in the topic of cryptocurrencies and blockchain technology.

We hope that you find the proceedings of CBT 2017 interesting and inspiring and that there will be follow-ups of the CBT workshop in the coming years.

Jordi Herrera-Joancomartí
Hannes Hartenstein

First International Workshop on Cryptocurrencies and Blockchain Technology CBT 2017

Program Committee Chairs

Hannes Hartenstein	Karlsruher Institut für Technologie, Germany
Jordi Herrera-Joancomartí	Universitat Autònoma de Barcelona, Spain

Program Committee

Rainer Böhme	Universität Innsbruck, Austria
Jeremy Clark	Concordia University, Canada
Christian Decker	Blockstream, USA
Joaquin Garcia-Alfaro	Telecom SudParis, Paris-Saclay University, France
Arthur Gervais	ETH, Switzerland
Man Ho Au	The Hong Kong Polytechnic University, SAR China
Ghassan Karame	NEC Research, Germany
Stefan Katzenbeisser	Technische Universität Darmstadt, Germany
Patrick McCorry	UCL, UK
Shin'ichiro Matsuo	BSafe.network and Keio University, Japan
Guillermo Navarro-Arribas	Universitat Autònoma de Barcelona, Spain
Mariusz Nowostawski	NTNU, Norway
Cristina Pérez-Solà	Universitat Autònoma de Barcelona, Spain
Roger Wattenhofer	ETH, Switzerland

Steering Committee

Rainer Böhme	Universität Innsbruck, Austria
Joaquin Garcia-Alfaro	Telecom SudParis, Paris-Saclay University, France
Hannes Hartenstein	Karlsruher Institut für Technologie, Germany
Jordi Herrera-Joancomartí	Universitat Autònoma de Barcelona, Spain

Additional Reviewers

Svetlana Abramova	Shinichi Miyazawa	Paulina Pesch
Sergi Delgado-Segura	Ken Naganuma	Kazue Sako
Michael Fröwis	Till Neudecker	Oliver Stengele

Contents

User Privacy

Applied Cryptography and Privacy

Consensus and Smart Contracts

Smart Contracts and Blockchain Identity